Deutscher Bundestag **Drucksache 19/12280**
19. Wahlperiode 12.08.2019

Antwort
der Bundesregierung

auf die Kleine Anfrage der Abgeordneten Dr. Konstantin von Notz, Agnieszka Brugger, Tabea Rößner, weiterer Abgeordneter und der Fraktion BÜNDNIS 90/DIE GRÜNEN
– Drucksache 19/11755 –

IT-Sicherheit durch mehr Transparenz und Standardisierung bei Zählweisen und Klassifizierungen von Angriffen

Vorbemerkung der Fragesteller

Zur Erlangung eines präzisen und faktenbasierten Lagebildes und zu den Grundlagen guten Regierens auch im Feld der IT-Sicherheit gehört es nach Ansicht der Fragesteller, möglichst eindeutige, transparente und nachvollziehbare Kennzahlen zur Nachzeichnung der Entwicklung im Bereich von IT-Angriffen zu erreichen. Nur auf der Grundlage faktenbasierter und nachvollziehbarer Darstellungen kann auch der Deutsche Bundestag zu problem- und sachbezogenen Diskussionen hinsichtlich seiner Kontroll- und Regulierungsaufträge in dieser für die Sicherheit der Bevölkerung zentralen Thematik gelangen.

Auf die Notwendigkeit klarer Definitionen und Zuständigkeiten bei der Abwehr von IT-Angriffen wurde wiederholt, auch in parlamentarischen Initiativen (vgl. beispielsweise Forderung h des Antrags der Fraktion BÜNDNIS 90/ DIE GRÜNEN „IT-Sicherheit stärken, Freiheit erhalten, Frieden sichern“ auf Bundestagsdrucksache 19/1328) hingewiesen. An der gängigen Praxis der pauschalisierenden Veröffentlichung von zum Teil extrem hohen oder auch niedrigen Zahlen ohne nähere Erläuterung von deren Zustandekommen (vgl. beispielsweise die Meldung der Bundesregierung, www.heise.de/newsticker/meldung/Ueber-47-Millionen-IT-Angriffe-auf-die-Bundeswehr-im-Jahr-2016-3595632.html) bestehen mit Blick auf die Notwendigkeit einer differenzierten und zutreffenden Einschätzung dieser komplexen Risiken durch die Öffentlichkeit aus Sicht der Fragesteller erhebliche Zweifel (Hinweise dazu etwa unter www.defenseone.com/ideas/2018/09/cyberspace-governments-dont-know-how-count/151629/?oref=d-river).

Vorbemerkung der Bundesregierung

Der von den Fragestellern verwendete Begriff „Hackback“ wird von der Bundesregierung konzeptionell nicht verwendet, weder für Aktivitäten der Cyber-Abwehr noch der Cyber-Verteidigung. Der Beantwortung dieser Kleinen Anfrage

---

Die Antwort wurde namens der Bundesregierung mit Schreiben des Bundesministeriums des Innern, für Bau und Heimat vom 8. August 2019 übermittelt.

Die Drucksache enthält zusätzlich – in kleinerer Schrifttype – den Fragetext.

legt die Bundesregierung insoweit die Begrifflichkeiten aus der Vorbemerkung der Bundesregierung zur Antwort auf die Kleine Anfrage der Fraktion der FDP auf Bundestagsdrucksache 19/2645 zugrunde.

1. Welche Stellen sind innerhalb der Bundesregierung und der ihr nachgeordneten Behörden mit der Klassifizierung und der Abwehr von IT-Angriffen beschäftigt (bitte im Einzelnen aufschlüsseln)?

Die Abwehr von IT-Angriffen einschließlich deren Klassifizierung ist eine Aufgabe, die jeder Betreiber von Netzen und IT-Systemen im Rahmen seiner Regelaufgaben wahrnimmt. Hierzu gibt es teilweise eigene Organisationsbereiche, wie beispielsweise der militärische Organisationsbereich Cyber- und Informationsraum im Geschäftsbereich des Bundesministeriums für Verteidigung.

Eine besondere Rolle kommt dem Bundesamt für die Sicherheit in der Informationstechnik (BSI) zu, das im Rahmen seines gesetzlichen Auftrags (§ 3 Absatz 1 Nummer 1 des Gesetzes über das Bundesamt für Sicherheit in der Informationstechnik – BSIG) für die Abwehr von Gefahren für die Sicherheit der Informationstechnik des Bundes insgesamt zuständig ist. Hierunter fällt auch die Abwehr von IT-Angriffen und deren Klassifizierung. Das BSI arbeitet dabei eng mit den behördlichen Auftragsdatenverarbeitern (u. a. ITZBund, BWI) und kommerziellen Dienstleistern/Providern zusammen.

Gemäß § 4 Absatz 2 Nummer 2 BSIG hat das BSI Bundesbehörden unverzüglich über die sie betreffenden Informationen und die in Erfahrung gebrachten Zusammenhänge zu unterrichten.

Das Bundesamt für Verfassungsschutz (BfV) ist bei der Abwehr von IT-Angriffen gemäß § 3 Absatz 1 des Gesetzes über die Zusammenarbeit des Bundes und der Länder in Angelegenheiten des Verfassungsschutzes und über das Bundesamt für Verfassungsschutz (BVerfSchG) zuständig für die Sammlung und Auswertung von Informationen über nachrichtendienstlich gesteuerte sowie extremistisch bzw. terroristisch motivierte IT-Angriffe.

Das BfV unterrichtet im Rahmen seiner Aufgabenerfüllung betroffene Bundesbehörden unverzüglich, sobald Erkenntnisse über einen möglichen oder versuchten bzw. erfolgten IT-Angriff vorliegen.

Ergänzend werden Betroffenen entsprechende Daten zum Schutz ihrer IT-Systeme zur Verfügung gestellt, die ein Erkennen und ggf. Abwehren des Angriffs ermöglichen.

Das Bundeskriminalamt (BKA) und die Bundespolizei (BPOL) sind im Rahmen der bestehenden Aufgaben auch zuständig für die Klassifizierung und Abwehr von IT-Angriffen.

Im Geschäftsbereich des Bundesministeriums der Verteidigung (BMVg) nimmt gemäß § 1 Absatz 1 des Gesetzes über den militärischen Abschirmdienst (MAD-Gesetz) der Militärische Abschirmdienst diese Aufgabe wahr.

Der Bundesnachrichtendienst (BND) sammelt im Rahmen seiner Zuständigkeiten Informationen über IT-Angriffe und wertet diese aus.

2. Welches Bundesministerium hat eine federführende bzw. koordinierende Funktion bei der Klassifizierung und der Abwehr von IT-Angriffen, und auf welchem Weg findet die Koordination zwischen den verschiedenen, mit der Thematik betreuten Bundesministerien statt?

Die Koordination zu Fragen der Klassifizierung und der Abwehr von IT-Angriffen erfolgt im Rahmen der ressortübergreifenden Arbeitsgruppe Informationssicherheitsmanagement (AG ISM). Für die Arbeit der AG ISM ist kein Ministerium federführend; koordinierende Aufgaben nimmt das Bundesministerium des Innern, für Bau und Heimat (BMI) wahr.

3. Welche Bundesministerien und nachgeordneten Bundesbehörden veröffentlichten (in Pressestatements der Hausleitungen usw.) in den zurückliegenden fünf Jahren eigene Zahlen zu Angriffen auf ihre eigenen IT-Systeme, IT-Netze, Infrastrukturen oder die IT-Systeme Dritter bzw. auf die IT-Infrastruktur der Bundesregierung insgesamt (bitte im Einzelnen auflisten)?

4. In wie vielen dieser Fälle erfolgten diese Veröffentlichungen auf Anweisung oder in Absprache mit einem der Bundesministerien (bitte entsprechend unterscheiden, welche, und Hintergrund darlegen)?

Wegen des Sachzusammenhangs werden die Fragen 3 und 4 gemeinsam beantwortet.

Das BSI veröffentlicht Zahlen zu Angriffen auf die IT-Infrastruktur der Bundesregierung insgesamt im jährlichen Bericht „Die Lage der IT-Sicherheit in Deutschland“: www.bsi.bund.de/DE/Publikationen/Lageberichte/lageberichte_node.html.

Im Geschäftsbereich des BMVg wurden im Rahmen von zwei Veröffentlichungen zur angefragten Thematik und zur auftretenden Häufigkeit Stellung bezogen:

1. Grundsatzartikel (aus 4/2018)
   www.bmvg.de/de/aktuelles/die-bedrohung-aus-dem-cyber-raum-fuer-die-bundeswehr-bleibt-konkret-23430
2. Veröffentlichung im Rahmen Y- Das Magazin der Bundeswehr (3/2019).
   Die Inhalte von Veröffentlichungen zur Thematik Angriff auf eigene IT-Infrastrukturen im Geschäftsbereich des Bundesministeriums der Verteidigung werden grundsätzlich mit den zuständigen Fachstellen des Bundesministeriums der Verteidigung abgestimmt.

Das Bundeskriminalamt (BKA) veröffentlicht jährlich das Bundeslagebild Cybercrime, in dem zu Straftaten und Phänomenen im Bereich Cybercrime berichtet wird. Die Lagebilder sind abrufbar unter: www.bka.de/DE/AktuelleInformationen/StatistikenLagebilder/Lagebilder/Cybercrime/cybercrime_node.html. Das BKA veröffentlicht zudem anlassbezogen Warnhinweise.

Die Bundespolizei (BPOL) veröffentlichte in den Jahresberichten 2017 S. 37 (1. November 2018) und 2018 S. 84 (17. Juli 2019) Zahlen zu den in Frage 3 angeführten Sachverhalten.

Die genannten Lageberichte, Lagebilder und Presseveröffentlichung werden regelmäßig zwischen den Geschäftsbereichen und den jeweiligen Fachaufsichtsressorts abgestimmt.

5. Welche Gefahrenstufen unterscheidet die Bundesregierung für das Vorliegen von Zugriffsversuchen, wie sind diese im Einzelnen definiert und kann die Bundesregierung eine für die Ressorts unterscheidbare Aufschlüsselung der jeweiligen Jahresstatistik nach Gefahrenstufen, wie etwa eine Antwort der Bundesregierung auf eine Frage des Abgeordneten Alexander Graf Lambsdorff (vgl. Bundestagsdrucksache 19/2922, Frage 87, S. 65) nach Ansicht der Fragesteller suggeriert, vorlegen?

Für die Behörden des Bundes klassifiziert die Allgemeine Verwaltungsvorschrift (AVV) über das Meldeverfahren gemäß § 4 Absatz 6 BSIG acht Gefährdungskategorien für die Informationstechnik (vgl. Anlage 1 der AVV) und orientiert sich dabei am Gefährdungskatalog der IT-Grundschutz-Kataloge sowie der ISO 27005; vgl. hierzu: www.verwaltungsvorschriften-im-internet.de/bsvwvbund_08122009_IT5606000111.htm.

Sofern bei einem IT-Vorfall eine unmittelbare Gefahr für die Sicherheit der Informationstechnik des Bundes nicht ausgeschlossen werden kann, sind die Behörden des Bundes gem. der o. g. AVV zur sofortigen Meldung (SOFORT-Meldung) der für die Abwehr von Gefahren für die Sicherheit in der Informationstechnik erforderlichen Informationen (insbesondere zu Sicherheitslücken, Schadprogrammen, erfolgten oder versuchten Angriffen auf die Sicherheit in der Informationstechnik und der dabei beobachteten Vorgehensweise) an das BSI verpflichtet. Dieses nimmt unverzüglich eine Bewertung der übermittelten Informationen vor.

Kann eine unmittelbare Gefahr für die Sicherheit der Informationstechnik des Bundes ausgeschlossen werden, erfolgt durch die Behörden monatlich eine gesammelte Meldung über die relevanten Informationen an das BSI (STATISTISCHE Gesamtmeldung). Eine Aufschlüsselung für die Ressorts ist hinsichtlich der SOFORT-Meldungen sowie der monatlichen Statistik-Meldungen derzeit technisch nicht vorgesehen.

Das BfV unterscheidet bei seinen Analysen nachrichtendienstlicher Cyberangriffe zwischen Zugriffsversuchen und tatsächlich erfolgten Zugriffen.

Die Antwort zu Frage 87 auf Bundestagsdrucksache 19/2922 nimmt Bezug auf die Klassifizierung von Cyberabgriffen im Bereich des Bundesministeriums der Verteidigung und dessen Geschäftsbereich (Bundeswehr), insoweit handelt es sich hier um eine ressortinterne Regelung.

Die an ihren zentralen Internetübergängen durch die Sensorik erfassten unberechtigten oder mit Schadpotenzial behafteten Zugriffsversuche unterscheidet der Geschäftsbereich des Bundesministeriums der Verteidigung nach den Gefahrenstufen „gering" und „hoch". Dabei werden Zugriffsversuche als „hoch" bewertet, die ein hohes Schadenspotenzial gehabt hätten, wenn keine präventiven technischen IT-Sicherheitsmaßnahmen durchgeführt worden wären. „Hoch" lässt damit also keinen Rückschluss auf die Schadenseintrittswahrscheinlichkeit zu und impliziert insbesondere nicht, dass ein Schaden tatsächlich eingetreten wäre.

Alle anderen über die Sensorik erfassten Zugriffsversuche werden mit „gering" bewertet. Damit ergibt sich auch die Möglichkeit eine Aufschlüsselung der jeweiligen Jahresstatistik nach Gefahrenstufen vorzunehmen.

Darüber hinaus meldet das Bundesministerium der Verteidigung und dessen Geschäftsbereich gemäß dem Meldeverfahren § 4 Absatz 6 BSIG.

6. In welcher Hinsicht haben sich konkret zwischen 2016 und 2017 aufgrund welcher Überlegungen und Vorgänge die Vorgaben für die statistische Zählweise als auch die Bewertungen für die Gefahrenstufe verändert (vgl. ebd.)?

Die Allgemeine Verwaltungsvorschrift über das Meldeverfahren gemäß § 4 Absatz 6 BSIG gilt seit ihrem Inkrafttreten im Jahr 2009 unverändert (vgl. Antwort zu Frage 5).

Für das BMVg und seinen Geschäftsbereich wurde eine Anpassung aufgrund von Erfahrungswerten und Überlegungen, wie auch von den Fragestellern in der Vorbemerkung angestellt, der bisherigen Regelungen und der Differenzierung nach Gefahrenstufen „hoch“ und „niedrig“ vorgenommen (vgl. Antwort zu Frage 5). Im Rahmen der statistischen Zählweise werden die Zahlen für Zugriffsversuche auf die im Ausland eingesetzten IT-Systeme nicht mehr gesondert ermittelt.

7. Hält die Bundesregierung die derzeitig genutzten Definitionen für ausreichend ausdifferenziert, um der Problematik angemessen zu begegnen?

Die Bundesregierung hält die getroffenen Regelungen, insbesondere die in der Allgemeinen Verwaltungsvorschrift über das Meldeverfahren gemäß § 4 Absatz 6 BSIG getroffene Klassifizierung, grundsätzlich für ausreichend. Bei Eintritt definierter herausgehobener Fälle werden diese gemäß BSIG zusätzlich individuell und einzelfallbezogen sorgfältig bearbeitet, um dem Problem angemessen zu begegnen.

8. Über welche Zahlen verfügt die Bundesregierung bezüglich Angriffen der Gefahrenstufe sog. Advanced Persistent Threats (APT) auf Bundesministerien oder Behörden in ihrem Geschäftsbereich (bitte im Einzelnen aufschlüsseln)?

Die Bundesregierung führt keine Statistiken zur Anzahl von APT-Angriffen.

9. Besteht für die Erkennung, Zählung und deren Definition bzw. Klassifizierung als IT-Angriff eine übergeordnete und/oder abgestimmte, für alle Bundesministerien und Bundesbehörden geltende Vorgehensweise oder gar Erlasslage?

   Wenn ja, welche konkret, und welche Informationen sind zu jedem Angriff aufzuzeichnen?

   Wenn nein, warum nicht?

Für die Erkennung, Zählung und deren Definition/ Klassifizierung als IT-Angriff gilt die Allgemeine Verwaltungsvorschrift über das Meldeverfahren gemäß § 4 Absatz 6 BSIG.

Der Umfang der bei einem IT-Vorfall dem BSI mitzuteilenden Informationen ist in Anlage 2 der vorgenannten AVV niedergelegt; vgl. hierzu: www.verwaltungs vorschriften-im-internet.de/pdf/BMI-IT5-20091208-SF-A002.pdf.

Im Übrigen wird auf die Antwort zu Frage 5 verwiesen.

10. Besteht aus Sicht der Bundesregierung eine (beispielsweise durch eine solche Erlasslage ermöglichte) Vergleichbarkeit zwischen Angriffen (Quantität und Qualität) auf einzelne Bundesministerien und Bundesbehörden?

Die Vergleichbarkeit der gemeldeten Vorfälle ist basierend auf der Allgemeinen Verwaltungsvorschrift über das Meldeverfahren gemäß § 4 Absatz 6 BSIG grundsätzlich gegeben.

11. Besteht für die Erkennung, Zählung und Definition bzw. Klassifizierung als IT-Angriff eine zwischen einzelnen oder mehreren Behörden des Bundes und der Länder abgestimmte Vorgehensweise, und wenn nein, warum nicht?

Auf die Antwort zu Frage 9 wird verwiesen.

Für die gemeinsame Abwehr von IT-Angriffen auf Bund und Länder hat der IT-Planungsrat ein verbindliches Meldeverfahren zum Informationsaustausch über IT-Sicherheitsvorfälle im VerwaltungsCERT-Verbund (VCV) beschlossen: www.it-planungsrat.de/SharedDocs/Sitzungen/DE/2017/Sitzung_24.html?pos=5.

12. Sollte es die in Frage 9 erfragte, übergeordnete und/oder abgestimmte, für alle Bundesbehörden geltende Vorgehensweise oder gar Erlasslage für die Erkennung, Zählung und deren Definition bzw. Klassifizierung als IT-Angriff nicht geben, gibt es zumindest für die innerhalb des Cyberabwehrzentrums (CAZ) zusammenarbeitenden Bundesministerien und Behörden hinsichtlich IT-Angriffen einheitliche Definitionen?

    Falls nicht, was hat die Bundesregierung bislang unternommen, um die unterschiedlichen Definitionen anzugleichen?

Die Bundesregierung verwendet als Rahmenvorgabe die in der Antwort zu Frage 9 angeführte Allgemeine Verwaltungsvorschrift über das Meldeverfahren gemäß § 4 Absatz 6 BSIG. Es steht den Behörden darüber hinaus frei, eigene für ihren spezifischen Aufgabenbereich erforderliche Definitionen zu treffen. Eine Vereinheitlichung aller Definitionen ist schon allein aufgrund der unterschiedlichen Zuständigkeiten der Behörden weder erforderlich noch zielführend.

13. Besteht für die Erkennung, Zählung und Definition bzw. Klassifizierung als IT-Angriff eine zwischen einzelnen oder mehreren Behörden europäischer Mitgliedstaaten oder in Organisationen wie der NATO abgestimmte Vorgehensweise, und wenn nein, warum nicht?

14. Wird die Bundesregierung sich für eine stärkere Klassifizierung und/oder Standardisierung einsetzen?

    Falls ja, welche Pläne gibt es hierfür konkret?

    Falls nein, warum nicht, und wird hierfür keine Notwendigkeit gesehen?

Wegen des Sachzusammenhangs werden die Fragen 13 und 14 gemeinsam beantwortet.

Die Kooperationsgruppe gemäß Artikel 11 der Richtlinie (EU) 2016/1148 des Europäischen Parlaments und des Rates vom 6. Juli 2016 über Maßnahmen zur Gewährleistung eines hohen gemeinsamen Sicherheitsniveaus von Netz- und Informationssystemen in der Union (NIS-Richtlinie) hat ein gemeinsames Dokument über eine „Cybersecurity Incident Taxonomy“ erarbeitet und im Juli 2018 veröffentlicht (abrufbar unter http://ec.europa.eu/newsroom/dae/document.cfm?doc_id=53646).

Die Kooperationsgruppe besteht aus Vertretern der EU-Mitgliedstaaten, der Europäischen Kommission und der Europäischen Agentur für Netz- und Informationssicherheit (ENISA). Gemäß dem in der NIS-Richtlinie, insbesondere in Artikel 11 Absatz 3 Buchstabe b niedergelegten Mandat der Kooperationsgruppe wird die Bundesregierung sich auch weiterhin für den Austausch von bewährten Verfahren über den Informationsaustausch im Zusammenhang mit der Meldung von Sicherheitsvorfällen einsetzen.

Für die Mitgliedstaaten der EU werden durch die ENISA entsprechende Empfehlungen veröffentlicht.

In der NATO gibt es derzeit keine verbindliche Vorgehensweise. Für die Bundesregierung und die übrigen Alliierten sind Fragen der Cyber-Sicherheit eine zuvorderst nationale Prärogative. Die NATO bietet hierfür eine Plattform für Konsultationen, Koordinierung und gegenseitige Unterstützung zwischen den Alliierten. Die Bundesregierung erachtet die bestehende Vorgehensweise als derzeit angemessen.

15. Hat es zwischen Behörden des Bundes jemals eine Diskussion und/oder eine Verständigung über eine entsprechende Matrix im Umgang mit der Erkennung, Definition bzw. Klassifizierung und der Zählung von IT-Angriffen gegeben, und wenn ja, wann, in welchem Rahmen (etwa im CAZ, während einer Sitzung der IMK usw.), welchen Inhalts und mit welchem Ergebnis (ggf. bitte entsprechende Handlungsanweisungen bzw. Erlasse etc. beifügen)?

Auf die Antwort zu Frage 9 wird verwiesen.

16. Plant die Bundesregierung eine entsprechende übergreifende oder zumindest für einzelne Behörden vorzunehmende Vereinheitlichung und/oder Standardisierung in der Klassifizierung und Zählung von IT-Angriffen, und wenn nein, warum nicht?

Es besteht seitens der Bundesregierung derzeit keine konkrete Planung zur Veränderung bei der Klassifizierung und Zählung von IT-Angriffen. Eine Fortentwicklung ist jederzeit möglich und das Verfahren dazu bereits in der Verwaltungsvorschrift definiert.

Im Übrigen wird auf die Antwort zu Frage 9 verwiesen.

17. Welche Formen von IT-Vorfällen (z. B. Pings, Port-Scans, E-Mails mit Schadprogrammen, Vireninfektionen etc.) werden in den unterschiedlichen Behörden für die Zählung berücksichtigt (bitte im Einzelnen aufzählen), und welche Risikoerwägungen liegen diesen Einordnungen jeweils zugrunde?

Auf die Antwort zu Frage 9 wird verwiesen.

18. Handelt es sich bislang im Schwerpunkt allein um die Zählung von durch Anti-Viren-Schutzmaßnahmen erfasste Schadprogramme (vgl. etwa BSI-Bericht von 2017 www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Lageberichte/Lagebericht2017.pdf?__blob=publicationFile&v=4), und wie werden diese Schadprogramme gezählt (z. B. Zählung je tatsächlich oder potentiell erreichtem E-Mail-Account oder Zählung nur ein Mal pro aufgefundenem, unterscheidbarem Schadprogramm etc.)?

Die statistische Erfassung von IT-Vorfällen beschränkt sich nicht nur auf von durch Anti-Viren-Schutzmaßnahmen erfasste Schadprogramme. Die vollständige Liste zu erfassender IT-Vorfälle ist in der Anlage 1 der Allgemeinen Verwaltungsvorschrift über das Meldeverfahren gemäß § 4 Absatz 6 BSIG aufgeführt; vgl. hierzu: www.verwaltungsvorschriften-im-internet.de/BMI-IT5-20091208-SF-A001.htm.

19. Zählen Spam-Mails und/oder Phishing-Mails nach wie vor als (einzeln zu erfassende) IT-Angriffe, und wenn ja, bei welchen Behörden?

Grundsätzlich sind weder Spam-Mails noch Phishing-Mails gemäß der Allgemeinen Verwaltungsvorschrift über das Meldeverfahren gemäß § 4 Absatz 6 BSIG zu erfassen. Wird jedoch deutlich, dass entsprechende E-Mails im Zusammenhang mit einem IT-Vorfall stehen, werden sie in der Regel gemeldet. Den Behörden steht es darüber hinaus frei, für eigene Zwecke derartige Zählungen durchzuführen. Sie gehen allerdings nicht in die offiziellen Zählstatistiken ein.

20. Zählen groß angelegte Angriffe, die über lange Zeiträume (Wochen oder Monate) durchgeführt werden, als einzelne IT-Angriffe, oder werden diese mehrfach erfasst?

    Wie wurde beispielsweise der Angriff auf die Netze des Deutschen Bundestages in der ersten Hälfte des Jahres 2015 gezählt?

Soweit diese groß angelegten Angriffe als zusammengehörig erkannt werden, werden sie als ein IT-Angriff statistisch erfasst, unabhängig von der zeitlichen Erstreckung des Angriffs oder der Vorfallsbearbeitung. Insbesondere wurde auch bei dem Angriff auf das Netz des Bundestages so verfahren.

21. In welcher Form werden durch IT-Angriffe ausgelöste Schäden und Beeinträchtigungen ermittelt und erfasst?

Im Rahmen der Ausführung der Allgemeinen Verwaltungsvorschrift über das Meldeverfahren gemäß § 4 Absatz 6 BSIG werden abstrakt die Auswirkungen auf die Informationen bzw. die Informationstechnik erfasst. Konkrete finanzielle oder personelle Aufwände zur Eindämmung bzw. Beseitigung der IT-Angriffe werden nicht systematisch erfasst.

22. Bestehen einheitliche Regeln dazu, in welcher Form, welchem Umfang und innerhalb welcher Frist die von IT-Angriffen betroffenen Bundesbehörden über diese in Kenntnis gesetzt werden müssen?

Grundsätzlich unterrichten sich Behörden im Rahmen der vertrauensvollen Zusammenarbeit unverzüglich, sobald Erkenntnisse über einen möglichen oder versuchten bzw. erfolgten IT-Angriff vorliegen.

Im Übrigen wird auf die Antwort zu Frage 1 verwiesen.

23. Teilt die Bundesregierung die Ansicht der Fragesteller, dass Begrifflichkeiten wie „Cyberangriff/Cyberattacke“ zu unspezifisch sind, um ein genaues Lagebild als Grundlage für Abwehrmaßnahmen etc. zu bekommen?

Basierend auf der Allgemeinen Verwaltungsvorschrift über das Meldeverfahren gemäß § 4 Absatz 6 BSIG werden IT-Vorfälle durch die Stellen des Bundes über die bloße Charakterisierung als „Cyberangriff/Cyberattacke“ hinaus detaillierter differenziert.

Im Übrigen wird auf die Antwort zu Frage 9 verwiesen.

24. Hat die Bundesregierung eine Position zur Frage, ob die Stärkung der IT-Sicherheit eine zentrale Bedingung für das Gelingen der gesellschaftlichen Gestaltung der Digitalisierung, für die Schaffung von Vertrauen in digitale Angebote und Infrastrukturen, für den Erhalt von Freiheit sowie für die Sicherung von Frieden ist und es bezüglich der Stärkung der IT-Sicherheit, der Zusammenarbeit der involvierten Bundesministerien und Behörden sowie der Härtung digitaler Infrastrukturen erheblicher weiterer Anstrengungen bedarf, um der verfassungsrechtlich gebotenen Schutzverantwortung für die Vertraulichkeit und Integrität informationstechnischer Systeme und dem Grundrecht auf Privatheit der Kommunikation gerecht zu werden?

Wenn nein, warum nicht?

Die Bundesregierung ist der Auffassung, dass die IT-Sicherheit eine der zentralen Voraussetzungen für eine erfolgreiche Digitalisierung ist. Weitere in der Frage genannte Aspekte, wie Vertrauen in digitale Angebote und Infrastrukturen oder Erhalt von Freiheit, sind eine Folge und hängen auch von mehr Faktoren als nur der IT-Sicherheit ab.

Die IT-Sicherheit ist ein fortwährendes Anliegen der Bundesregierung, das sie seit der Verbreitung der IT in Staat, Wirtschaft und Gesellschaft intensiv berücksichtigt. Bereits 1991 hat sie das Bundesamt für die Sicherheit in der Informationstechnik ins Leben gerufen.

Zu den jüngsten Maßnahmen zur Verbesserung der Cyber- und IT-Sicherheit zählen u. a. das IT-Sicherheitsgesetz aus 2015, mit deutlichen Anforderungen an die Verbesserung der IT-Sicherheit bei Kritischen Infrastrukturen, die „Cyber-Sicherheitsstrategie für Deutschland 2016“ mit übergreifenden Zielstellungen für alle Bereiche und Akteure in der IT-Sicherheit und das sogenannte NIS-Richtlinien-Umsetzungsgesetz, in dem auch die Anbieter „Digitaler Dienste“ zur Umsetzung von Maßnahmen zur Gewährleistung von IT-Sicherheit auf dem jeweiligen Stand der Technik verpflichtet werden.

Das für diese Legislatur geplante IT-Sicherheitsgesetz 2.0 zielt u. a. darauf ab, die von Wirtschaftsunternehmen zu treffenden Schutzmaßnahmen für ihre IT-Systeme kontinuierlich auf einem der Bedrohungslage angemessenen Stand zu halten, ein IT-Sicherheitskennzeichen einzuführen und den digitalen Verbraucherschutz zu stärken. Hinzu kommen zahlreiche Aktivitäten aller Ressorts der Bundesregierung mit denen die Cyber- und IT-Sicherheit kontinuierlich angepasst und verbessert wird.

25. Wie ist der derzeitige Stand der Erarbeitung des seit langem angekündigten sogenannten IT-Sicherheitsgesetzes 2.0, und wann wird die Bundesregierung den Gesetzentwurf dem Deutschen Bundestag zur parlamentarischen Beratung vorlegen?

Der Gesetzentwurf für ein IT-Sicherheitsgesetz 2.0 befindet sich in der Ressortabstimmung. Er wird dem Deutschen Bundestag zur parlamentarischen Beratung nach Abschluss des in der Gemeinsamen Geschäftsordnung der Bundesministerien (GGO) vorgesehenen Verfahrens vorgelegt.

26. Wird die Frage der Erfassung und Klassifizierung von IT-Angriffen im „IT-Sicherheitsgesetz 2.0“ eine Rolle spielen?

Die Bundesregierung nimmt keine Stellung zu Gesetzentwürfen, die sich in der Abstimmung befinden.

27. Gibt es von Seiten der Bundesregierung Überlegungen, die Zuständigkeit für die IT-Sicherheit aus dem Bundesministerium des Innern, für Bau und Heimat herauszulösen und einem anderen Ressort zu übertragen?

    Falls ja, welchem?

    Falls nein, warum nicht?

Es bestehen keine dahingehenden Überlegungen, die Zuständigkeiten für die IT-Sicherheit des Bundesministeriums des Innern, für Bau und Heimat zu verändern.

28. Gibt es von Seiten der Bundesregierung Überlegungen, die Zusammenarbeit im Cyberabwehrzentrum (CAZ) auf eine neue rechtliche Grundlage zu stellen und personell auszubauen?

    Wenn ja, wie konkret?

    Falls nicht, wird die bisherige Form der Zusammenarbeit und der rechtlichen Grundlagen sowie der personellen Ausstattung als gut bewertet?

29. Ist das Cyberabwehrzentrum (CAZ) aktuell rund um die Uhr besetzt und hinsichtlich anwesender Personen arbeitsfähig?

    Falls nein, zu welchen Zeiten ist das CAZ besetzt?

30. Plant die Bundesregierung, das Cyberabwehrzentrum (CAZ) mit einem Koordinator auszustatten, der im Falle eines möglichen Angriffs die Zuständigkeiten der Behörden koordiniert, wie dies der Inspekteur Cyber- und Informationsraum, Generalleutnant Ludwig Leinhos angeregt hatte (vgl.: www.tah.de/welt/afp-news-single/cyber-inspekteur-brauchen-koordinator-im-nationalen-cyber-abwehrzentrum.html)?

31. Welche Aufgaben sollen der Bundeswehr in Zukunft im Rahmen des Cyberabwehrzentrum (CAZ) zufallen?

Wegen des Sachzusammenhangs werden die Fragen 28 bis 31 gemeinsam beantwortet.

Beim Cyber-Abwehrzentrum handelt es sich um eine Informations-, Koordinations- und Kooperationseinrichtung von Bundesbehörden mit Sicherheitsaufgaben, die keine eigenständige Behörde ist. Die am Cyber-Abwehrzentrum beteiligten Behörden bringen sich im Rahmen ihrer jeweiligen Zuständigkeiten sowie des ansonsten für sie geltenden Rechts ein.

Das Cyber-Abwehrzentrum unterliegt einem kontinuierlichen Weiterentwicklungsprozess. Im nächsten Schritt wird das Cyber-Abwehrzentrum u. a. das Cyber-Lagebild und die Risikobewertung zu Cyber-Gefahren weiter optimieren sowie eine intensivere Koordinierung der operativen Zusammenarbeit realisieren. Durch verbesserten Informationsaustausch in Verbindung mit der bereits bestehenden 24/7-Erreichbarkeit kann zudem schneller und koordinierter auf Cyber-Angriffe reagiert werden. Die Zusammenarbeitsprozesse der am Cyber-Abwehrzentrum beteiligten Behörden werden deutlich optimiert.

32. Gibt es von Seiten der Bundesregierung Überlegungen, das Bundesamt für Sicherheit in der Informationstechnik bzw. Teile davon, angesichts der nach Ansicht der Fragesteller immer wieder auftretenden Interessenkonflikte, unabhängig zu stellen, auch, um es in seiner Beratungsfunktion gegenüber Bürgerinnen und Bürgern wie Unternehmen zu stärken?

    Wenn nein, warum nicht?

Die Bundesregierung beabsichtigt nicht, das Bundesamt für Sicherheit in der Informationstechnik (BSI) als unabhängige Stelle einzurichten (vgl. auch Antwort zu Frage 24f der Kleinen Anfrage der Fraktion DIE LINKE. auf Bundestagsdrucksache 19/1867).

Das BSI ist als Cyber-Sicherheitsbehörde auf eine enge Zusammenarbeit mit den klassischen Sicherheitsbehörden angewiesen und diese benötigen wiederum die Expertise des BSI. Diese Zusammenarbeit lässt sich in geeigneter Weise durch die Einbettung des BSI in die bestehenden Strukturen der Bundesregierung gewährleisten.

33. Welche Stelle koordiniert aktuell die notwendige Gesamtbeobachtung hybrider Bedrohungen (hybrid threats), führt die Erkenntnisse zusammen und berichtet dazu innerhalb der Bundesregierung?

Innerhalb der Bundesregierung ist das BMI federführend für den Themenkomplex „hybride Bedrohungen“ zuständig. Im Rahmen dieser Zuständigkeit führt das BMI Erkenntnisse zusammen und berichtet dazu innerhalb der Bundesregierung.

34. Gibt es von Seiten der Bundesregierung Überlegungen, neue Zuständigkeiten für die systematische Beobachtung hybrider Bedrohungen zu schaffen, um so mögliche Angriffe, insbesondere auf zivile und für das staatliche Wohl relevante digitale sowie kritische Infrastrukturen, identifizieren und abwehren zu können?

    Falls ja, welche konkret?

    Falls nein, werden die derzeit zur Verfügung stehenden Strukturen als ausreichend betrachtet?

Die Erkennung von Bedrohungen für die öffentliche Sicherheit und Ordnung ist Aufgabe der Sicherheitsbehörden von Bund und Ländern. Um die verschiedenen Erkenntnisse zu einer hybriden Bedrohung zusammenzuführen, existieren bereits Zusammenarbeitsstrukturen wie u. a. das Cyberabwehrzentrum. Ob die zur Verfügung stehenden Zusammenarbeitsstrukturen als ausreichend betrachtet werden können oder daneben neue Zuständigkeiten erforderlich sind, wird regelmäßig von der Bundesregierung überprüft.

35. Gibt es von Seiten der Bundesregierung Überlegungen, eine eigenständige, fachlich unabhängige Organisationseinheit zur Bewertung einer etwaigen Zurechenbarkeit von Angriffen (Attribution) zu schaffen?

    Falls ja, welche konkret?

    Falls nicht, warum wird dies als nicht notwendig erachtet?

Eine eigenständige, fachlich unabhängige Organisationeinheit wird von der Bundesregierung nicht angestrebt. Die Attribution von Cyberangriffen erfolgt aktuell durch die jeweils zuständigen Behörden, die sich abstimmen. Der Abstimmungsprozess wird derzeit überprüft.

36. Hält die Bundesregierung an ihren Plänen, eine gesetzliche Grundlage zur Ermöglichung digitaler Gegenschläge, sogenannter Hackbacks, fest, und wer soll nach den bisherigen Plänen der Bundesregierung auf welcher Rechtsgrundlage die politische wie rechtliche Verantwortung für derartige Angriffe übernehmen?

37. Welche konkreten Pläne und Überlegungen haben die Bundesregierung oder einzelne Bundesministerien hierzu in den vergangenen zwölf Monaten angestellt, welche Treffen haben hierzu zwischen verschiedenen Bundesministerien stattgefunden, welche Papiere wurden hierzu erarbeitet, welche Gutachten, beispielsweise zu verfassungs-, europa- und/oder völkerrechtlichen Fragen, bei wem in Auftrag gegeben und welche „Stufenpläne“ erstellt (vgl. www.tagesschau.de/investigativ/seehofer-cyberabwehr-103.html)?

38. Gibt es nach Kenntnis der Bundesregierung eine im Koalitionsvertrag zwischen CDU, CSU und SPD festgehaltene, diesbezügliche Vereinbarung oder anderweitige, zwischenzeitlich erfolgte Einigung bezüglich des weiteren Vorgehens?

39. Ist von Seiten der Bundesregierung diesbezüglich eine Änderung des Grundgesetzes geplant, und wann will die Bundesregierung dem Parlament einen entsprechenden Vorschlag vorlegen?

40. Ist nach Ansicht der Bundesregierung ein Mandat des Deutschen Bundestages für einen digitalen Gegenschlag („Hackback“) notwendig?

    Falls nicht, wie begründet die Bundesregierung diese Rechtsauffassung?

41. Wie bewertet die Bundesregierung die Gefahr, dass durch Angriffe und das Eindringen in fremde Systeme („Hackbacks“) Eskalationsspiralen im digitalen Raum befördert werden können?

Wegen des Sachzusammenhangs werden die Fragen 36 bis 41 gemeinsam beantwortet.

Die im Zusammenhang mit Maßnahmen der aktiven Cyber-Abwehr aufgeworfenen Fragestellungen werden derzeit von der Bundesregierung geprüft. Diese Prüfungen sind noch nicht abgeschlossen. Im Rahmen dieser Prüfungen fanden und finden auch Ressortbesprechungen statt. Im Rahmen dieser Prüfungen wurden von der Bundesregierung keine wissenschaftlichen Gutachten bei Dritten in Auftrag gegeben.

Darüber hinaus wird auf die Antworten der Bundesregierung zu den Fragen 1 bis 3 sowie 22 der Kleinen Anfrage der Fraktion der FDP auf Bundestagsdrucksache 19/5472 verwiesen.

Der Koalitionsvertrag zwischen CDU, CSU und SPD ist öffentlich einsehbar.

42. Hat die Bundesregierung einen multidisziplinären Prüfprozess nach Artikel 36 des Zusatzprotokolls vom 8. Juni 1977 zu den Genfer Abkommen vom 12. August 1949 über den Schutz der Opfer internationaler bewaffneter Konflikte (ZP I) der Genfer Konvention für Einsätze offensiver Fähigkeiten der Bundeswehr zum Wirken im Cyber-Raum und deren Vereinbarkeit mit dem geltenden humanitären Völkerrecht durchgeführt, und wenn ja, mit welchem Ergebnis?

    Falls nein, warum nicht?

Einsätze von Cyber-Fähigkeiten der Bundeswehr folgen nur in Übereinstimmung mit den geltenden Rechtsgrundlagen. Dazu wird jeder Einsatz rechtlich geprüft und durch Rechtsberater begleitet. Cyber-Wirkmittel wurden als Mittel der Kriegsführung in Überstimmung mit Artikel 36 des Zusatzprotokoll I zu den Genfer Abkommen auf ihre Vereinbarkeit mit dem humanitären Völkerrecht geprüft. Cyber-Wirkmittel sind demnach kein per se unzulässiges Mittel der Kriegsführung. Ein konkreter Einsatz muss in Übereinstimmung mit den humanitär-völkerrechtlichen Vorgaben, insbesondere dem Unterscheidungsgebot, erfolgen.

43. Sieht die Bundesregierung die Gefahr, wonach undifferenzierte, nicht näher erläuterte Angaben zu „millionenfachen Cyberangriffen“ (vgl. etwa die Zahlen aus der Antwort der Bundesregierung auf die Schriftliche Frage zur Bundeswehr, Quelle siehe Fragen 5 und 6) schon aufgrund etwa der fehlenden näheren Aufschlüsselung nach Gefahrenstufen geeignet sein können, mehr Verunsicherung statt Aufklärung der Öffentlichkeit zu bewirken, und wenn nein, warum nicht?

Im Geschäftsbereich des Bundesministeriums der Verteidigung findet eine Differenzierung sämtlicher IT-Vorfälle, die an den zentralen Internetübergängen durch die Sensorik erfasst werden, entlang der Gefahrenstufen „gering“ und „hoch“ statt.

Im Übrigen wird auf die Antwort zu Frage 9 verwiesen.

44. Hat die Bundesregierung eine Position zur Forderung des Inspekteurs Cyber- und Informationsraum der Bundeswehr, Generalleutnant Ludwig Leinhos nach Einrichtung eines so genannten „digitalen Verteidigungsfalles“, der unterhalb der Schwelle eines „klassischen Verteidigungsfalles“ anzusiedeln sei (vgl.: www.tah.de/welt/afp-news-single/cyber-inspekteur-brauchen-koordinator-im-nationalen-cyber-abwehrzentrum.html), und wenn ja, welche?

    a) Was genau ist nach Ansicht der Bundesregierung unter einem „digitalen Verteidigungsfall“ zu verstehen?

    b) Welche gesetzlichen Grundlagen bestehen nach Ansicht der Bundesregierung hierfür bzw. wären zu schaffen?

    c) Welche Voraussetzungen müssen erfüllt sein, dass es zur Ausrufung eines solchen „digitalen Verteidigungsfalles“ käme?

       Welche Kompetenzen und welche Rolle kämen jeweils dem Deutschen Bundestag, dem Bundesrat sowie der Bundesregierung zu?

    d) Plant die Bundesregierung hierzu Gesetzesinitiativen bzw. Änderungen des Grundgesetzes?

Die Fragen 44 und 44a bis 44d werden aufgrund ihres inhaltlichen Zusammenhangs zusammen beantwortet.

Der Begriff „digitaler Verteidigungsfall“ wird durch die Bundesregierung nicht verwendet, daher existiert hierfür keine festgelegte Definition. Er stellt keinen Rechtsbegriff dar, der an rechtliche Voraussetzungen anknüpft oder rechtliche Konsequenzen auslöst.

45. Ist aus Sicht der Bundesregierung der Übergang von der sogenannten Cyberabwehr zur „Cyberverteidigung“ ausreichend klar gesetzlich geregelt?

Wenn nein, wo besteht hier Nachsteuerungsbedarf?

Cyber-Abwehr und Cyber-Verteidigung sind sich ergänzende Mittel zum Erreichen von Cyber-Sicherheit und damit zwei stetig wahrzunehmende Aufgabenbereiche.

Im Falle eines bewaffneten Angriffs steht der Bundesrepublik Deutschland das Recht zu, sich zu verteidigen. Dies erlaubt eine Reaktion mit allen nach Maßgabe des Völkerrechts zulässigen militärischen Mitteln und umfasst auch den Einsatz von militärischen Cyber-Fähigkeiten. Auch in diesem Fall findet in Deutschland weiterhin zivile Cyber-Abwehr statt.



Satz: Satzweiss.com Print, Web, Software GmbH, Mainzer Straße 116, 66121 Saarbrücken, www.satzweiss.com
Druck: Printsystem GmbH, Schafwäsche 1-3, 71296 Heimsheim, www.printsystem.de
Vertrieb: Bundesanzeiger Verlag GmbH, Postfach 10 05 34, 50445 Köln, Telefon (02 21) 97 66 83 40, Fax (02 21) 97 66 83 44, www.betrifft-gesetze.de
ISSN 0722-8333